Final Exam — Solution Guide

MAT 200

There are seven questions, of varying point-value.
Each question is worth the indicated number of points.

1. *(15 points)* If X is uncountable and $A \subseteq X$ is countable, prove that $X - A$ is uncountable. What does this tell us about the set of irrational real numbers?

A set is called *countable* if it is either finite or denumerable. A set Y is countable if and only if there exists an injection $f : Y \to \mathbb{Z}^+$.

Our hypotheses say that A is countable and that X is uncountable. We now proceed via proof by contradiction. If $X - A$ were countable, there would be an injection $f : (X - A) \to \mathbb{Z}^+$. Since A is countable by hypothesis, there is certainly an injection $g : A \to \mathbb{Z}^+$. The function $h : X \to \mathbb{Z}^+$ defined by

$$h(x) = \begin{cases} 2g(x), & \text{if } x \in A \\ 2f(x) + 1, & \text{if } x \in (X - A) \end{cases}$$

would then be injective, sending distinct elements of A to distinct even integers and distinct elements of $X - A$ to distinct odd integers. Thus X would be countable, in contradiction to our hypothesis. This shows that $X - A$ must be uncountable.

As an application, we now consider the example given by $X = \mathbb{R}$ and $A = \mathbb{Q}$. Since Cantor proved that the set $\mathbb{R}$ of real numbers is uncountable, and since the set $\mathbb{Q}$ of rational number is countable, it follows that the set $\mathbb{R} - \mathbb{Q}$ of irrational real numbers is uncountable.

2. *(15 points)* Prove by induction that

$$\sum_{k=1}^{n} k^3 = \frac{(n+1)^2 n^2}{4}$$

for every positive integer n.

For any $n \in \mathbb{Z}^+$, let $P(n)$ be the statement that

$$\sum_{k=1}^{n} k^3 = \frac{(n+1)^2 n^2}{4}.$$

The base case $P(1)$ then says that

$$1^3 = \frac{2^2 \cdot 1}{4},$$

which is certainly true.

We now need to prove that $P(m) \Longrightarrow P(m+1)$ for any positive integer m. Thus, suppose that

$$\sum_{k=1}^{m} k^3 = \frac{(m+1)^2 m^2}{4}$$

holds for some positive integer m. It then follows that

$$\begin{aligned}
\sum_{k=1}^{m+1} k^3 &= \left(\sum_{k=1}^{m} k^3\right) + (m+1)^3 \\
&= \frac{(m+1)^2 m^2}{4} + (m+1)^3 \\
&= \frac{m^2(m+1)^2 + 4(m+1)(m+1)^2}{4} \\
&= \frac{(m^2+4m+4)(m+1)^2}{4} \\
&= \frac{(m+2)^2(m+1)^2}{4}
\end{aligned}$$

so we have shown that the statment $P(m+1)$ is a logical conseqence of the statement $P(m)$.

By the principle of induction, $P(n)$ therefore holds for all $n \in \mathbb{Z}^+$.

3. *(15 points)* Let X and Y be finite sets, with $|X| = n \geq 3$ and $|Y| = 3$. Compute

$$\left|\left\{ f : X \to Y \;\middle|\; f \text{ surjective } \right\}\right|.$$

Hint: How many f aren't surjective? Use the inclusion/exclusion principle.

Let y_j, $j = 1, 2, 3$, denote the three elements of Y, so that

$$Y = \{y_1, y_2, y_3\}.$$

For $j = 1, 2, 3$, let A_j be the set of all functions $f : X \to Y - \{y_j\}$. Thus

$$A_j = \{f : X \to Y \mid y_j \notin \vec{f}(X)\}.$$

We then have

$$A_1 \cup A_2 \cup A_3 = \{f : X \to Y \mid f \text{ is not surjective}\}.$$

Now

$$|A_j| = |Y - \{y_j\}|^{|X|} = 2^n$$

for each j. Similarly

$$|A_j \cap A_k| = 1$$

for each $j \neq k$, and

$$A_1 \cap A_2 \cap A_3 = \varnothing.$$

The inclusion/exclusion principle therefore implies that

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= \sum_j |A_j| - \sum_{j<k} |A_j \cap A_k| + |A_1 \cap A_2 \cap A_3| \\ &= 3 \cdot 2^n - 3 \end{aligned}$$

Since

$$|\{f : X \to Y\}| = |Y|^{|X|} = 3^n$$

we therefore have

$$\left|\left\{ f : X \to Y \;\middle|\; f \text{ surjective } \right\}\right| = 3^n - (3 \cdot 2^n - 3) = 3(3^{n-1} - 2^n + 1).$$

4. *(15 points)* Let A and B be distinct points in the plane. Assuming the axioms of Euclidean geometry, prove that the set

$$\mathbb{L} = \left\{ \mathsf{C} \in \text{Plane} \;\middle|\; |\mathsf{AC}| = |\mathsf{BC}| \right\}$$

is a line.

Hint: First show that there is a unique line ℓ through the mid-point of $\overline{\mathsf{AB}}$ which meets $\overleftrightarrow{\mathsf{AB}}$ in a right angle. Then show that $\mathbb{L} = \ell$.

By the ruler axiom, the segment $\overline{\mathsf{AB}}$ has a mid-point, which is the unique $\mathsf{M} \in \overleftrightarrow{\mathsf{AB}}$ with $|\mathsf{AM}| = |\mathsf{MB}|$. Choose a side of $\overleftrightarrow{\mathsf{AB}}$, which we treat as the interior of the straight angle $\angle AMB$. The protractor axiom then says that we can find a unique ray $\overrightarrow{\mathsf{MD}}$ on the chosen side of $\overleftrightarrow{\mathsf{AB}}$ such that $m\angle\mathsf{AMD} = \pi/2$. If $\mathsf{D}' \in \overleftrightarrow{\mathsf{MD}}$ is on the opposite side of $\overleftrightarrow{\mathsf{AB}}$ from D, we have $m\angle\mathsf{AMD} = m\angle\mathsf{AMD}' = m\angle\mathsf{BMD} = m\angle\mathsf{BMD}' = \pi/2$ by vertical and supplementary angles, so we would have therefore constructed exactly the same line $\overleftrightarrow{\mathsf{MD}}$ if we had instead chosen the opposite side of $\overleftrightarrow{\mathsf{AB}}$, or had interchanged A and B. The line $\ell = \overleftrightarrow{\mathsf{MD}}$ is therefore uniquely defined; it is usually called the perpendicular bisector of $\overline{\mathsf{AB}}$.

Let us next show that $\mathbb{L} \subseteq \ell$. If $\mathsf{C} \in \mathbb{L}$, then $|\mathsf{AC}| = |\mathsf{BC}|$, by the definition of $\mathbb{L}$. If $\mathsf{C} \in \overleftrightarrow{AB}$, we then have $\mathsf{C} = \mathsf{M}$, so $\mathsf{C} \in \ell = \overleftrightarrow{\mathsf{MD}}$, as claimed. Otherwise, the triangles $\triangle\mathsf{AMC}$ and $\triangle\mathsf{BMC}$ are well defined, as in each case the given vertices are not collinear. However, $|\mathsf{AC}| = |\mathsf{BC}|$, $|\mathsf{AM}| = |\mathsf{BM}|$ and $|\mathsf{MC}| = |\mathsf{MC}|$. Hence $\triangle\mathsf{AMC} \cong \triangle\mathsf{BMC}$ by the SSS congruence theorem. Therefore $m\angle\mathsf{AMC} = m\angle\mathsf{BMC}$. Since these angles are supplementary, we therefore have $m\angle\mathsf{AMC} = \pi/2$. Hence $\overleftrightarrow{\mathsf{MC}} = \ell$, and $\mathsf{C} \in \ell$. Thus $(\mathsf{C} \in \mathbb{L}) \Longrightarrow (\mathsf{C} \in \ell)$, and $\mathbb{L} \subseteq \ell$, as claimed.

We now show that $\ell \subseteq \mathbb{L}$. If $\mathsf{C} \in \ell$, either $\mathsf{C} = \mathsf{M}$, and hence $\mathsf{C} \in \mathbb{L}$, or else $\mathsf{C} \notin \overleftrightarrow{AB}$. In the latter case, $\triangle\mathsf{AMC}$ and $\triangle\mathsf{BMC}$ are then well defined. Moreover, $m\angle\mathsf{AMC} = m\angle\mathsf{BMC} = \pi/2$, since ℓ is perpendicular to $\overleftrightarrow{AB}$. Moreover, $|\mathsf{AM}| = |\mathsf{BM}|$ and $|\mathsf{MC}| = |\mathsf{MC}|$. Consequently, $\triangle\mathsf{AMC} \cong \triangle\mathsf{BMC}$ by the SAS congruence axiom. Hence $|\mathsf{AC}| = |\mathsf{BC}|$, and so $\mathsf{C} \in \mathbb{L}$. That is, $(\mathsf{C} \in \ell) \Longrightarrow (\mathsf{C} \in \mathbb{L})$, and $\ell \subseteq \mathbb{L}$.

Since $\mathbb{L} \subseteq \ell$ and $\ell \subseteq \mathbb{L}$, $\mathbb{L} = \ell$. In particular, $\mathbb{L}$ is a line, as claimed.

5. *(10 points)* Let $n \geq 2$ be an integer. Use modular arithmetic to show that

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

is always an integer, and is even if and only if $n \equiv 0$ or $1 \bmod 4$.

The question is equivalent to showing that

$$n(n-1) \equiv 0 \text{ or } 2 \bmod 4$$

for any integer n, and that

$$n(n-1) \equiv 0 \bmod 4$$

iff $n \equiv 0$ or $1 \bmod 4$.

Modulo 4, any integer n is congruent to 0, 1, 2, or 3. Let us tabulate the relevant products of remainders mod 4:

n	$n-1$	$n(n-1)$
0	3	0
1	0	0
2	1	2
3	2	2

Thus $n(n-1) \equiv 0$ or $2 \bmod 4$ for any n, and is $\equiv 0 \bmod 4$ if and only if $n \equiv 0$ or $1 \bmod 4$, exactly as claimed.

6. *(20 points)* (a) Use modular arithmetic to prove the following:

If n is an integer, and if n^2 is divisible by 5, then n is divisible by 5.

Hint: What is the contrapositive, in terms of congruence mod 5?

We must show that $(n \not\equiv 0 \bmod 5) \implies (n^2 \not\equiv 0 \bmod 5)$. Since any integer is congruent mod 5 to 0, 1, 2, 3, or 4, we merely need to make a table of squares, modulo 5:

n	n^2
0	0
1	1
2	4
3	4
4	1

By direct inspection, we conclude that $n^2 \not\equiv 0 \bmod 5$ whenever $n \not\equiv 0 \bmod 5$, as claimed.

(b) Use part (a) to prove that there is no rational number q with $q^2 = 5$. Conclude that $\sqrt{5} \notin \mathbb{Q}$.

Hint: If there were such a q, first argue that it could be expressed as a/b, where at least one of the integers a, b isn't divisible by 5.

Any rational number q may be expressed as a quotient a/b, where $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$, and by repeatedly cancelling common factors of 5, we may assume that at most one of a, b is divisible by 5. Now, having done this, let us assume our rational number q satisfies $q^2 = 5$. We then have $\frac{a^2}{b^2} = 5$, so that $a^2 = 5b^2$ and $a^2 \equiv 0 \bmod 5$. But, by part (a), this implies that $a \equiv 0 \bmod 5$. Hence $a = 5n$ for some $n \in \mathbb{Z}$, and

$$\frac{25n^2}{b^2} = \frac{a^2}{b^2} = 5$$

and hence $b^2 = 5n^2$. Thus $b^2 \equiv 0 \bmod 5$. and part (a), this implies that $b \equiv 0 \bmod 5$. That is, both a and b are divisible by 5, contradicting our assumption. Hence no such q exists; that is, $\sqrt{5}$ cannot be a rational number.

7. (*10 points*) Let X and Y be sets, and let $f : X \to Y$ be a function. For $a, b \in X$, define the expression

$$a \simeq b$$

to mean that

$$f(a) = f(b).$$

Prove that $\simeq$ is an equivalence relation on X.

We need to verify that $\simeq$ is

(R) reflexive:

(S) symmetric; and

(T) transitive.

Reflexive: Since $f(a) = f(a)$ for any $a \in X$, we always have $a \simeq a$. Thus $\simeq$ is reflexive.

Symmetric: If $f(a) = f(b)$, it follows that $f(b) = f(a)$. Thus $(a \simeq b) \implies (b \simeq a)$, and $\simeq$ is therefore symmetric.

Transitive: If $f(a) = f(b)$ and $f(b) = f(c)$, it follows that $f(a) = f(c)$. Thus $(a \simeq b \text{ and } b \simeq c) \implies (a \simeq c)$, and $\simeq$ is therefore transitive.

Since the relation $\simeq$ on X is reflexive, symmetric, and transitive, it follows that $\simeq$ is an equivalence relation.